CA Nimsoft Monitor

Guia do Usuário da Detecção

v7.5

Março de 2014

Avisos legais

Este sistema de ajuda online (o “Sistema”) destina-se somente para fins informativos e está sujeito a alteração ou revogação por parte da CA a qualquer momento.

O Sistema não pode ser copiado, transferido, reproduzido, divulgado, modificado nem duplicado, por inteiro ou em parte, sem o prévio consentimento por escrito da CA. O Sistema contém informações confidenciais e propriedade da CA e está protegido pelas leis de direitos autorais dos Estados Unidos e por tratados internacionais. O Sistema não pode ser divulgado nem usado para nenhum fim que não seja o permitido em um acordo separado entre você e a CA, o qual rege o uso do software da CA ao qual o Sistema está relacionado (o “Software da CA”). Tal acordo não é modificado de nenhum modo pelos termos deste aviso.

Não obstante o que foi estabelecido acima, se você for um usuário licenciado do Software da CA, poderá fazer uma cópia do Sistema para uso interno por você e seus funcionários, contanto que todas as legendas e avisos de direitos autorais da CA estejam afixados à cópia reproduzida.

O direito de fazer uma cópia do Sistema está limitado ao período de vigência no qual a licença do Software da CA permanece em pleno vigor e efeito. Em caso de término da licença, por qualquer motivo, você fica responsável por garantir à CA, por escrito, que todas as cópias, parciais ou integrais, do Sistema foram destruídas.

DENTRO DO PERMITIDO PELA LEI APLICÁVEL, A CA FORNECE O SISTEMA “COMO ESTÁ”, SEM GARANTIA DE NENHUM TIPO, INCLUINDO, SEM LIMITAÇÃO, QUAISQUER GARANTIAS IMPLÍCITAS DE COMERCIABILIDADE E ADEQUAÇÃO A UM DETERMINADO FIM OU NÃO VIOLAÇÃO. EM NENHUMA OCASIÃO, A CA SERÁ RESPONSÁVEL POR QUAISQUER PERDAS OU DANOS, DIRETOS OU INDIRETOS, DO USUÁRIO FINAL OU DE QUALQUER TERCEIRO, RESULTANTES DO USO DESTE SISTEMA INCLUINDO, SEM LIMITAÇÃO, LUCROS CESSANTES, PERDA DE INVESTIMENTO, INTERRUPÇÃO DOS NEGÓCIOS, PERDA DE DADOS OU ATIVOS INTANGÍVEIS, MESMO QUE A CA TENHA SIDO EXPRESSAMENTE ADVERTIDA SOBRE A POSSIBILIDADE DE TAIS PERDAS E DANOS.

O fabricante deste Software é a CA.

Fornecido nos termos de “Direitos restritos”. O uso, a duplicação ou a divulgação pelo Governo dos Estados Unidos está sujeito às restrições definidas nas seções 12.212, 52.227-14 e 52.227-19(c)(1) - (2) da FAR e na seção 252.227-7014(b)(3) da DFARS, conforme aplicável, ou seus sucessores.

Copyright © 2014 CA. Todos os direitos reservados. Todas as marcas comerciais, nomes comerciais, marcas de serviços e logotipos mencionados neste documento pertencem às respectivas empresas.

As informações legais sobre software de domínio público e de terceiros usado na solução do Nimsoft Monitor estão documentadas em *Licenças de Terceiros e Termos de Uso do Nimsoft Monitor (*http://docs.nimsoft.com/prodhelp/en_US/Library/Legal.html*).*

Entrar em contato com a CA

Entrar em contato com a CA Support

Para sua conveniência, a CA Technologies oferece um site onde é possível acessar as informações necessárias a seus produtos da CA Technologies para escritório doméstico, pequena empresa e corporativos. Em http://ca.com/support, é possível acessar os seguintes recursos:

- Informações para contato online e telefônico, assistência técnica e atendimento ao cliente
- Informações sobre fóruns e comunidades de usuário
- Downloads de produto e documentação
- Políticas e diretrizes de CA Support
- Outros recursos úteis adequados ao seu produto

Fornecendo comentários sobre a documentação do produto

Enviar comentários ou perguntas sobre a documentação de produtos da Nimsoft da CA Technologies para nimsoft.techpubs @ ca.com.

Se desejar fornecer comentários sobre a documentação geral dos produtos da CA Technologies, responda nossa breve pesquisa do cliente, disponível no site de CA Support, encontrado em http://ca.com/docs.

Histórico de revisões do documento

Versão	Data	Alterações
7.5	Março de 2014	Atualizações secundárias do NMS 7.5.
7.1	Dezembro de 2013	Revisado para o NMS 7.1: ■ Atualizado para incluir a detecção de dispositivos IPv6.
7.0	Setembro de 2013	Revisado para o NMS 7.0: ■ Adição da correlação de dispositivos. ■ Nova fila probe_discovery. ■ Alterações ao Assistente de detecção. ■ Eliminação das interfaces do usuário do probe de detecção. ■ Melhoria no conteúdo.
6.5	Abril de 2013	Primeira edição do guia, abrangendo o Nimsoft Discovery implementado no NMS versão 6.5.

Índice

Capítulo 1: Arquitetura de detecção 7

Componentes da detecção 9
Considerações de detecção 10
Pré-requisitos e plataformas suportadas 11

Capítulo 2: Configurando a detecção 13

Implantar o NMS 13
Configurar filas de detecção 15
Iniciar o Assistente de detecção 16
    Criar perfis de autenticação 17
    Definir intervalos 22
    Detecção programada 24
Executar a importação com base em arquivo 25
Exibir sistemas detectados 26

Apêndice A: Configuração avançada 29

Executando o discovery_server em um robô que não o hub principal 29
Configurando o tamanho máximo da pilha do Java 30
    Servidor de detecção 30
    Agente de detecção 31
Referência de importação com base em arquivo 32
    Esquema de arquivo XML 34

Capítulo 1: Arquitetura de detecção

A tarefa da *detecção* automática é localizar e registrar todos os dispositivos e computadores disponíveis em um ambiente de TI gerenciado. Quando vários registros de detecção correspondem a um único dispositivo, esses registros são reconhecidos pela *correlação* de dispositivos. A lista de registros de dispositivos pode ser complementada com a importação de dispositivos *com base em arquivos* XML ou com a entrada manual do dispositivo.

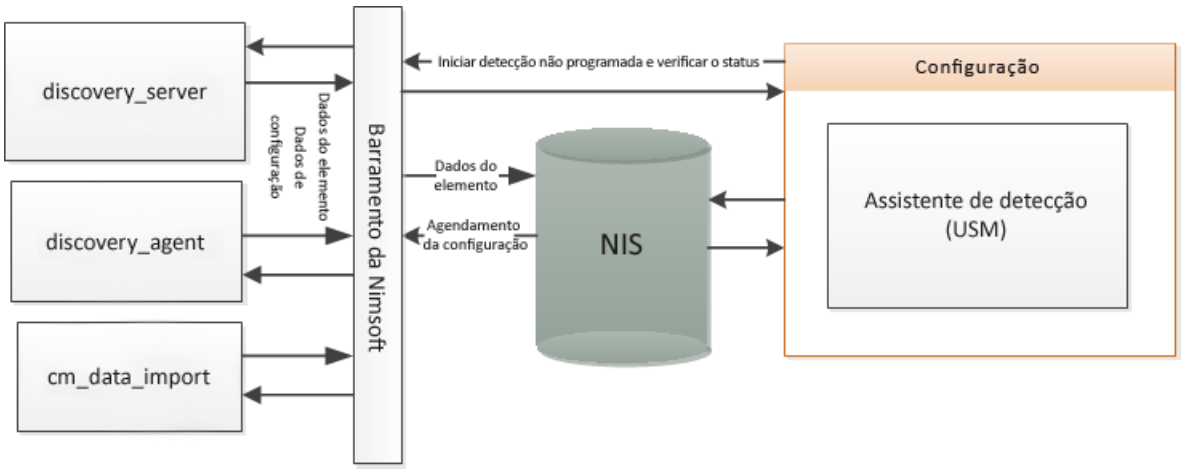
Uma parte importante de monitoramento de TI é a criação e manutenção de uma lista exata dos dispositivos presentes em seu ambiente de TI. A tarefa da *detecção* automática é localizar e listar todos os dispositivos e computadores disponíveis em um ambiente de TI gerenciado.

Após a instalação do CA Nimsoft Unified Management Portal (UMP), o Assistente de detecção inicia automaticamente e solicita a configuração e execução da detecção. O assistente permite que você especifique as credenciais de autenticação e defina os intervalos de endereços IP a serem verificados. A Detecção localiza praticamente todos os recursos conectados à rede e fornece informações detalhadas sobre o tipo de dispositivo, a configuração e os ativo/dados de inventário. Com ICMP, ARP, DNS, SNMP (versões 1, 2 e 3), WMI, SSH e NetBIOS, a detecção localiza uma ampla variedade de dispositivos e informações do dispositivo.

A lista de dispositivos, conhecida como *Inventário*, pode ser complementada com a importação de dispositivos com base em arquivos XML ou com a entrada manual do dispositivo. Quando vários registros de detecção correspondem a um único dispositivo, esses registros são reconhecidos pela correlação de dispositivos.

Para manter seu inventário, é possível executar novamente a detecção a qualquer momento, modificando as credenciais e os intervalos, conforme necessário. Você também pode programar a execução da detecção para execução a intervalos regulares.

Este diagrama ilustra o fluxo de dados entre os principais componentes da detecção automática:



Esta seção contém os seguintes tópicos:

Componentes da detecção (na página 9)
Considerações de detecção (na página 10)
Pré-requisitos e plataformas suportadas (na página 11)

Componentes da detecção

Todos os componentes da detecção são incluídos em uma instalação básica do CA Nimsoft Monitor Server.

Assistente de detecção

As verificações de detecção são configuradas no Assistente de detecção. Para iniciar o assistente, abra o portlet USM (Unified Service Manager – Gerenciador de serviços unificados) no UMP e selecione **Ações**. Também é possível executar o assistente em qualquer nó do agente de detecção na árvore de detecção do USM.

O assistente permite configurar um dos seguintes métodos de detecção:

- A *detecção automática* preenche o inventário do dispositivo por meio da verificação da rede de acordo com perfis de autenticação e escopos de verificação configurados.
- A *importação com base em arquivo* importa uma lista composta por um ou mais hosts ou dispositivos de rede de um arquivo XML.

Mais detalhes sobre esses tópicos encontram-se na seção sobre o Assistente de detecção (na página 16).

Probe do servidor de detecção

Na maioria das instalações, o probe discovery_server é executado no hub principal. O probe executa estas principais tarefas:

- Configura agentes de detecção e coleta seus status.
- Coleta informações sobre a infraestrutura da Nimsoft: hubs, robôs, probes, pacotes, sistemas ou dispositivos monitorados, subsistemas ou itens monitorados, e métricas monitoradas.
- Coleta dados de dispositivos dos probes que publicam informações de detecção.
- Aplica regras de correlação para associar novos registros de dispositivos, quando apropriado, a registros de dispositivos mestres já existentes. Um exemplo é a representação exata de dispositivos com várias páginas iniciais (aqueles com várias interfaces de rede).

As informações coletadas pelo probe discovery_server são salvas no banco de dados do NIS e usadas por outros componentes na solução Nimsoft Monitor.

Observação: mesmo que não haja probes discovery_agent implantados, o probe discovery_server continua sendo necessário para gerar os dados exigidos por outros componentes no Nimsoft Monitor.

Probe do agente de detecção

O probe discovery_agent verifica a rede de TI por meio de pings e consultas a dispositivos de acordo com as máscaras de sub-rede/os intervalos, os perfis de credenciais e os perfis selecionados. Esses parâmetros de verificação são configurados no Assistente de detecção.

Importação de dados do CM

Esse probe processa um arquivo XML que descreve os hosts e dispositivos, e adiciona essas informações ao inventário do dispositivo. Esse probe normalmente encontra-se no mesmo local que o servidor de detecção. Quando você executa a importação com base em arquivo do Assistente de detecção, a Importação de dados do CM executa o trabalho.

Componentes adicionais que têm função na detecção:

Fila probeDiscovery

Essa fila no hub principal coleta de dados de detecção que são processados pelo servidor de detecção. Nos hubs secundários, configure as filas probe_discovery para coletar dados e encaminhá-los ao hub principal. Consulte Configurar a fila discovery_probe (na página 15).

NIS (Nimsoft Information Store - Armazenamento de informações do Nimsoft)

O NIS é o banco de dados que contém todos os dados persistentes no Nimsoft Monitor, o que inclui dados de detecção.

Outros probes do Nimsoft Monitoring

Todos os probes de monitoramento fornecem informações sobre os sistemas monitorados para o servidor de detecção. Vários desses probes publicam diretamente na fila probeDiscovery. Esses probes de monitoramento ajudam a complementar a detecção automática.

Considerações de detecção

- O recurso *Topologia e análise de causa raiz* do Nimsoft Monitor usa os dados fornecidos pela detecção para deduzir a estrutura da rede e o moldá-lo. O modelo pode ser exibido no portlet Visualizador de relacionamentos no UMP. Consulte mais informações sobre os tópicos de topologia e análise de causa raiz no Guia do Usuário de Topologia e Análise de Causa Raiz.

- Os dispositivos são importados no Nimsoft por meio da importação com base em arquivos não estão refletidas na topologia nem na análise da causa raiz. A topologia depende das informações do SNMP coletadas pelo agente de detecção sobre os dispositivos.

Pré-requisitos e plataformas suportadas

- A Detecção 7.x requer o NMS 7.x.
- O Servidor de detecção 7.x funciona somente com Agentes de detecção 7.x. O servidor de detecção gera um alarme ao localizar agentes de detecção anteriores à versão 7.0.
- O Servidor de detecção 7.x não coleta resultados de detecção de agentes de detecção anterior à versão 7.0.

Para as plataformas do sistema NMS suportadas, consulte a Matriz de suporte de compatibilidade do Nimsoft Monitor para obter mais detalhes.

Capítulo 2: Configurando a detecção

Veja como o processo de detecção funciona:

1. Você instala o NMS, que inclui os componentes necessários para a detecção.
2. Se a instalação do NMS incluir hubs secundários, você deve configurar as filas *probeDiscovery* para que as mensagens de probe_discovery cheguem ao hub principal. Consulte Configurar filas de detecção (na página 15).
3. Você instala o UMP, que inclui o Assistente de detecção.
4. Após a instalação do UMP, o Assistente de detecção é iniciado no USM e conduz pelo processo de configuração da detecção. Você vai:
   a. Criar perfis de autenticação (na página 17)
   b. Definir intervalos (na página 22) (conjuntos ou intervalos de endereços IP e máscaras IP que definem e impõem o escopo da detecção)
   c. Agendar a detecção (na página 24).
5. Para ampliar a detecção automática, você pode preparar um arquivo XML com informações de dispositivos e importá-las no inventário de dispositivos (opcional). Consulte Executar a importação com base em arquivo (na página 25).
6. Quando a detecção for concluída, você poderá visualizar os computadores e dispositivos detectados na rede. Consulte Visualizar sistemas detectados (na página 26).

Implantar o NMS

Os componentes (probes) necessários para detecção são implantados no hub principal com uma instalação básica do CA Nimsoft Monitor:

- Servidor de detecção
- Agente de detecção
- Importação de dados do CM

Lembre-se das informações a seguir se desejar modificar a implantação de probe de detecção padrão:

- Para o mínimo de detecção, apenas o probe discovery_server é necessário. Nenhuma verificação é executada na rede.
- Para adicionar a verificação de rede, implante o probe discovery_agent no hub principal do NMS ou em outro lugar.
- Para obter a detecção ideal em ambientes maiores, é possível implantar mais de um agente de detecção. Alguns usuários, especialmente os provedores de serviço e aqueles que têm redes muito grandes, acham útil implantar vários agentes de detecção em diversos locais.

  A detecção de uma rede grande pode ser dividida com base nos limites administrativos por estas razões:

  - Para fornecer acesso a diferentes partes da rede a usuários diferentes.
  - Em situações em que não há conectividade direta com dispositivos em um site remoto devido às restrições de firewall ou a NAT (Network-Address Translation – conversão de endereços de rede). Para que a detecção seja eficiente, implante agentes de detecção de forma que cada um detecte uma parte exclusiva da rede.
- Observe que o protocolo WMI só é suportado por probes discovery_agent em execução nos sistemas Windows.

Dica: o Agente de detecção requer acesso SNMP somente leitura aos dispositivos de rede. Para simplificar a configuração da detecção, deve-se considerar a configuração do máximo de dispositivos de rede possível para usar uma sequência de caracteres de comunidade "universal" somente leitura (recomenda-se o uso de SNMP versão 3, em vez das versões 1 e 2c). Por exemplo, é possível definir credenciais somente leitura (get-only) como **nms_get_only**. Em seguida, configure todos os dispositivos possíveis para permitir o acesso SNMP somente leitura por meio dessas credenciais. Isso minimiza a quantidade de tentativas de credenciais de autenticação do SNMP em nós de rede, e simplifica amplamente a configuração da detecção.

Configurar filas de detecção

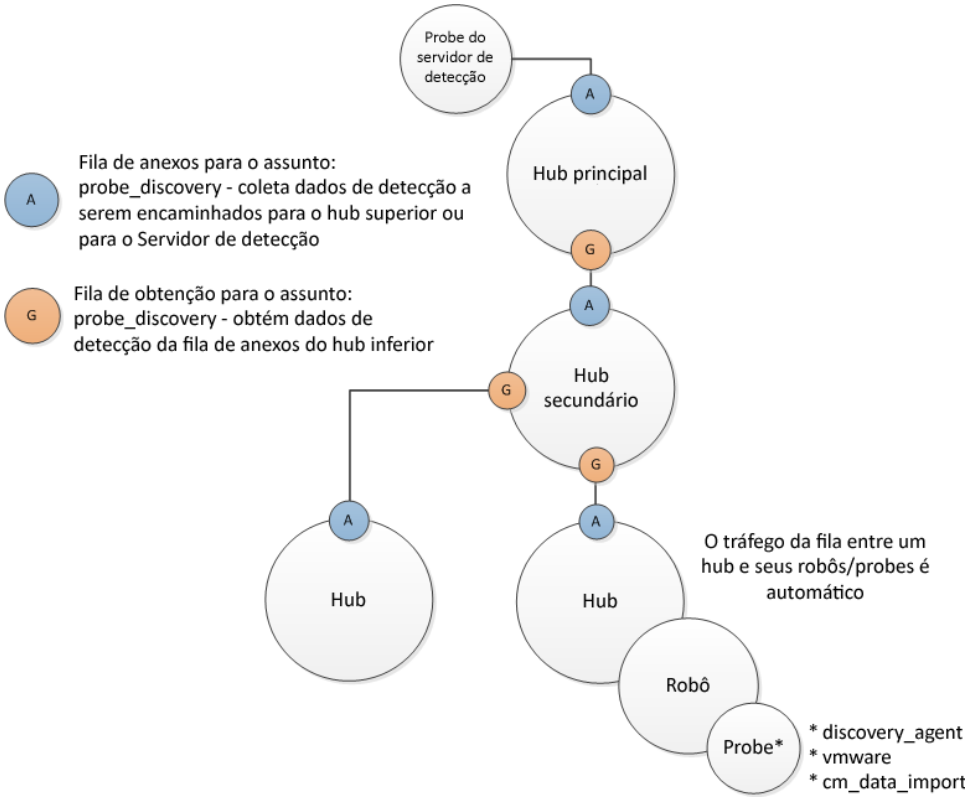
Se todos os probes do processo de detecção estiverem implantados em um único hub, a comunicação dos dados de detecção será configurada automaticamente. No entanto, se os probes de detecção estiverem implantados em *outros* hubs que não o hub que hospeda o probe discovery_server, você deverá garantir que os dados podem fluir desses hubs até o hub principal.

Isso é feito por meio da configuração de filas que manipulam o *probe_discovery*. Você configurará filas de *anexos* (que coletam mensagens) no hub principal e nos hubs que hospedam os seguintes probes:

- discovery_agent
- vmware 5.10 ou posterior
- cm_data_import (esse probe geralmente é implantado com o probe discovery_serve no hub principal)

Você configurará uma fila de *obtenção* correspondente (que recupera mensagens da fila de anexos) no hub principal e em qualquer hub que precise transferir as mensagens para outro hub.

A ilustração a seguir mostra onde as filas são obrigatórias.


Probe do servidor de detecção
A
Hub principal
G
A
Fila de anexos para o assunto: probe_discovery - coleta dados de detecção a serem encaminhados para o hub superior ou para o Servidor de detecção
G
Fila de obtenção para o assunto: probe_discovery - obtém dados de detecção da fila de anexos do hub inferior
Hub secundário
G
A
A
Hub
Hub
O tráfego da fila entre um hub e seus robôs/probes é automático
Robô
Probe*
* discovery_agent
* vmware
* cm_data_import

Para configurar as filas de detecção, siga estas etapas.

1. No Gerenciador de infraestrutura, identifique o hub no qual deseja criar uma fila. Expanda o nó do hub e clique duas vezes no probe do hub.
2. Clique na guia **Filas**.
3. Para configurar uma fila de *anexos*, clique em **Novo** e especifique:
   - **Ativo:** ativado
   - **Nome:** probeDiscovery
   - **Tipo:** selecione *anexo*
   - **Assunto:** selecione *probe_discovery*
4. Para configurar uma fila de *obtenção*, clique em **Novo** e especifique:
   - **Ativo:** ativado
   - **Nome:** probeDiscovery
   - **Tipo:** selecione *obter*
   - **Endereço:** selecione o endereço do hub que tem a fila de anexos
   - **Tamanho em massa:** especifique o número de mensagens a serem enviadas em conjunto (opcional; se você quiser que a fila execute uma grande quantidade de mensagens, o envio em massa pode melhorar o desempenho)

Depois de configurar todas as filas necessárias, execute uma verificação de detecção automática (no Assistente de detecção no USM) para confirmar que as filas estão em operação. Verifique a lista de dispositivos detectados. Além dos dispositivos locais, a lista também deve conter dispositivos que estão disponíveis apenas nos hubs secundários da infraestrutura.

Observação: a configuração da outras filas de alarmes, QoS (Quality of Service – qualidade do serviço) e dados da linha de base é semelhante à configuração de filas de anexos e obtenção. O assunto muda conforme o tipo de dados a ser executado.

Dica: em implantações de pequeno e médio porte do NMS, um caractere curinga (*), que executa qualquer mensagem, pode simplificar a configuração de filas. Não recomendamos usar um caractere curinga em instalações de grande porte do NMS.

Iniciar o Assistente de detecção

Quando você abre o UMP (Unified Management Portal) pela primeira vez, ele é aberto no portlet Gerenciador de serviços unificados e o Assistente de detecção é iniciado automaticamente.

Depois que você abrir o UMP pela primeira vez, poderá iniciar o Assistente de detecção manualmente se quiser executar a detecção ou alterar as configurações de detecção. É possível iniciar o Assistente de detecção a partir do nó Inventário ou a partir do menu **Ações**.

Observação: o Assistente de detecção não será executado após uma atualização do CA Nimsoft Monitor se houver intervalos que definem os endereços IP *excluídos*. Você deve optar por aceitar o prompt do sistema para excluir intervalos excluídos ou removê-los manualmente do banco de dados antes de a detecção ser executada.

Siga estas etapas:

1. Passe o cursor ou clique no nome de um agente de detecção ou intervalo na árvore.

   Os agentes de detecção são indicados pelo ícone de lupa ( ) e os intervalos são indicados pelo ícone de rede ( ).
2. Clique no ícone de engrenagem ( ) à direita do nome do agente de detecção ou do intervalo na árvore ou escolha **Assistente de detecção** no menu **Ações**.

   Observação: a opção de menu **Assistente de detecção** só é ativada quando você clica em um agente de detecção ou intervalo na árvore.

Criar perfis de autenticação

As guias WMI, Linux/Unix e SNMP permitem criar, editar, exibir e excluir perfis de autenticação da detecção. Um perfil de autenticação contém informações de credenciais necessárias para que a detecção acesse e colete informações sobre os sistemas de computador e dispositivos na sua rede.

É possível criar um ou mais perfis de autenticação em cada uma das guias WMI, Linux/Unix e SNMP.

Observação: a criação de perfis de autenticação não é obrigatória para a detecção. No entanto, somente a detecção de IP é usada quando não houver nenhum outro perfil de autenticação e as informações sobre os sistemas detectados podem ser limitadas.

Selecione a guia WMI, Linux/Unix ou SNMP e clique no nome de um perfil de autenticação no painel esquerdo para exibir as suas propriedades no painel da direita.

Para modificar um perfil de autenticação já existente, selecione-o e edite os campos conforme necessário e clique em **Salvar**. Para excluir um perfil de autenticação, clique no ícone da lixeira ( ) ao lado do nome do perfil no painel esquerdo e, em seguida, clique em **Salvar**.

Siga estas etapas para criar um perfil de autenticação:

1. Clique em **Novas credenciais** no painel esquerdo.
2. Digite as informações em todos os campos obrigatórios.

   Os campos obrigatórios estão destacados em vermelho.
3. Clique em **Avançar**.

   As informações inseridas serão salvas ao clicar em **Avançar** e percorrer o Assistente de detecção.

Linux/Unix

Os perfis de autenticação Linux/Unix usam SSH ou Telnet para acessar e detectar sistemas Linux e Unix.

Descrição

Nome do perfil de autenticação.

ID

Esse campo somente leitura é a ID do sistema da Nimsoft para este perfil de autenticação, atribuída quando o perfil foi salvo. Ele identifica o perfil com exclusividade para que seja reutilizado em outras áreas do USM que fazem referência a perfis de autenticação.

Usuário

O nome do usuário.

Senha

A senha do usuário. Marque a caixa de seleção **Mostrar novas senhas** para ver o texto conforme você for digitando.

SSH ou Telnet

Selecione o protocolo de comunicação a ser usado, SSH (Secure Shell) ou Telnet (sem autenticação segura ou criptografia).

Observação: o Agente de detecção usa a autenticação de *senha* para se conectar a um dispositivo de destino através de SSH. O Agente de detecção não pode se comunicar com um dispositivo em que o SSH está configurado para outros métodos de autenticação, como interativa por teclado. O Agente de detecção também não oferece suporte à autenticação de chave pública nem à autenticação desafio-resposta.

SNMP

A detecção do CA Nimsoft oferece suporte para as versões 1, 2c e 3 do protocolo SNMP. O SNMP v3 adiciona recursos de segurança que não existem na v1 e na v2c. Consequentemente, os campos de configuração do perfil de autenticação no Assistente de detecção relacionados a segurança e privacidade (criptografia) só ficam ativos quando **3** é selecionado no menu suspenso **Versão**.

Sugerimos as seguintes práticas recomendadas:

- Crie um conjunto mínimo de perfis de autenticação do SNMP que irá, no todo, fornecer ao SNMP o acesso a todos os dispositivos de rede e hosts que oferecem suporte ao SNMP.
- Configure o máximo possível de dispositivos de rede para usar credenciais “universais” de somente leitura. Por exemplo, é possível definir uma credencial somente leitura (get-only) como **nms_get_only**. Em seguida, configure todos os dispositivos possíveis para permitir o acesso SNMP somente leitura por meio da credencial. Isso minimiza o número de tentativas de credenciais de autenticação do SNMP que devem ser feitas em nós da rede e simplifica a configuração de detecção.
- Se houver dispositivos que aceitem credenciais SNMP exclusivas, crie um perfil de autenticação para cada uma delas. É possível especificar uma porta exclusiva dentro do intervalo de 1 a 65535 para o perfil. Se nenhuma porta for especificada, a porta padrão 161 será usada.

Campo (SNMP v1 ou v2)	Obrigatório	Descrição
Descrição	Sim	Nome do perfil de autenticação

ID		Esse campo somente leitura é a ID do sistema da Nimsoft para este perfil de autenticação, atribuída quando o perfil foi salvo. Ele identifica o perfil com exclusividade para que seja reutilizado em outras áreas do USM que fazem referência a perfis de autenticação.
Versão	Sim	A versão do SNMP suportada pelo dispositivo monitorado. Quando versão 1 ou 2 é selecionada, somente o campo Comunidade fica ativado.
Comunidade	Sim	A sequência de caracteres SNMP. Selecione **Mostrar novas senhas** para ver o texto conforme você for digitando. É válido observar que essa sequência de caracteres é enviada pela rede em texto não criptografado como parte de solicitações SNMP v1 ou v2c, o que pode representar um risco à segurança.

Campo (SNMP v3)	**Obrigatório**	**Descrição**
Descrição	Sim	Nome do perfil de autenticação
ID		Esse campo somente leitura é a ID do sistema da Nimsoft para este perfil de autenticação, atribuída quando o perfil foi salvo. Ele identifica o perfil com exclusividade para que seja reutilizado em outras áreas do USM que fazem referência a perfis de autenticação.
Versão	Sim	A versão do SNMP suportada pelo dispositivo monitorado. Há suporte para as versões 1, 2c e 3. Quando v3 é selecionada, outras campos de segurança e privacidade são ativados.
Senha	Consulte a observação.	A senha associada ao dispositivo SNMP v1/v2c ou ao usuário de SNMP v3. Selecione **Mostrar novas senhas** para ver o texto conforme você for digitando. **Observação**: esse campo será ativado e obrigatório se a segurança **AuthNoPriv** ou **AuthPriv** for selecionada. Consulte a descrição do campo Segurança a seguir.
Usuário	Sim	O nome do usuário de SNMP v3 utilizado para acessar o dispositivo monitorado. Obrigatório para todos os níveis de segurança SNMP v3. Consulte a descrição do campo Segurança a seguir.
Método	Sim	Método de criptografia SNMP v3, quando a segurança **AuthPriv** é selecionada (consulte a descrição do campo Segurança a seguir): ■ **Nenhum** ■ **MD5** - Algoritmo MD5 Message Digest (HMAC-MD5-96) ■ **SHA** - Algoritmo Secure Hash (HMAC-SHA-96)

Segurança	Sim	Nível de segurança do usuário de SNMP v3. Dependendo do nível de segurança selecionado, outros campos de segurança estarão ativados ou desativados. ■ **NoAuthNoPriv** - mensagens enviadas não autenticadas e não criptografadas ■ **AuthNoPriv** - mensagens enviadas autenticadas, mas não criptografadas ■ **AuthPriv** - mensagens enviadas autenticadas e criptografadas
Senha privada	Consulte a observação.	A senha de privacidade do SNMP v3 a ser usada se o nível de segurança **AuthPriv** for selecionado. Deve ter ao menos oito caracteres. Não confunda com a senha do usuário (autenticação). **Observação**: esse campo será ativado e obrigatório se a segurança **AuthPriv** for selecionada.
Protocolo privado	Consulte a observação.	Protocolo de privacidade (criptografia) SNMP v3 a ser usado. ■ **DES** (Data Encryption Standard - Padrão de Criptografia de Dados) ■ **AES** (Advanced Encryption Standard - Padrão de Criptografia Avançada) **Observação**: ativado e obrigatório se a segurança **AuthPriv** for selecionada.

WMI

A detecção da WMI (Windows Management Interface) verifica servidores e hosts que executam o Windows para coletar informações do sistema. A detecção da WMI é executada apenas nos agentes de detecção hospedados em sistemas Windows.

Descrição

Nome do perfil de autenticação.

ID

Esse campo somente leitura é a ID do sistema da Nimsoft para este perfil de autenticação, atribuída quando o perfil foi salvo. Ele identifica o perfil com exclusividade para que seja reutilizado em outras áreas do USM que fazem referência a perfis de autenticação.

Usuário

O nome do usuário, no formato **Domínio\nome de usuário**. **nome_do_usuário** e **endereço_IP/nome_do_usuário** também são permitidos.

Senha

Senha do usuário. Marque a caixa de seleção **Mostrar novas senhas** para ver o texto conforme você for digitando.

Definir intervalos

Use a guia Intervalos do Assistente de detecção para definir os intervalos, as máscaras ou os endereços de rede em que os dispositivos devem ser detectados. Pelo menos um intervalo de rede deve ser inserido para que a detecção seja executada.

É possível atribuir qualquer combinação de perfis de autenticação do SNMP, Linux/Unix e WMI a um intervalo. O processo de detecção registra *qualquer* dispositivo em um intervalo que responda a uma solicitação sobre qualquer protocolo, inclusive um simples ping ICMP. Isso significa que é possível incluir nós finais (como servidores, impressoras de rede, sistemas de armazenamento de rede ou estações de trabalho) em um intervalo, mesmo que eles não respondam a solicitações por meio de SNMP ou outros protocolos de gerenciamento.

Se nenhum perfil de autenticação estiver atribuído a um intervalo, a detecção básica é executada usando os protocolos que não exigem autenticação, mas a detecção pode não ser concluída, e as informações sobre os sistemas detectados são limitadas.

Práticas recomendadas para a criação de intervalos

Para cada agente de detecção, verifique os intervalos atribuídos para minimizar os tempos limite previsíveis. Para otimizar o desempenho e evitar entradas duplicadas, cada agente de detecção deve detectar uma parte exclusiva da rede.

Dicas para reduzir o tempo de execução da detecção:

- O agente de detecção tenta cada credencial em cada endereço IP e aguarda um aviso de tempo limite (ou êxito) após cada tentativa. Use uma única credencial em um intervalo que tem alta probabilidade de êxito imediato em seus nós para acelerar a detecção.
- Ao aplicar um perfil de autenticação a um intervalo, certifique-se de que a maioria, se não todos, dos dispositivos definidos por este intervalo aceita o perfil de autenticação.
- Se incluir dispositivos que não respondam a solicitações em nenhum protocolo de gerenciamento, coloque-os em um intervalo de detecção sem perfis de autenticação atribuídos ao intervalo.
- Se usar o SNMP para um dispositivo que aceite apenas sequências de caracteres da comunidade SNMP exclusivas, crie um intervalo de tipo **Único** e especifique o endereço IP do dispositivo. Atribua o perfil de autenticação correspondente ao intervalo.
- Ao usar o SNMP, para evitar interceptações/alertas de autenticação desnecessários, atribua apenas uma credencial de autenticação do SNMP por intervalo de detecção.

Criar um intervalo

Siga estas etapas:

1. Clique em **Novo intervalo**, no painel esquerdo da guia Intervalos.
2. Insira um nome para o intervalo.
3. Na seção Definição de intervalo, especifique a(s) área(s) de sua rede em que deseja executar a detecção:

   - **Máscara** - Máscara de bits de uma sub-rede usando a notação CIDR (Classless Inter-Domain Routing) com um endereço IPv4 de base e um prefixo de roteamento. Por exemplo, 195.51.100.0/24. O valor /24 refere-se a uma sub-rede de classe C de 256 endereços. Outros valores para referência: /30 (4 endereços) e /16 (65.536 endereços ou uma sub-rede de Classe B).

     Observação: ao digitar uma máscara de sub-rede, o número dos endereços IP que a máscara representa é exibido (que é o número de hosts efetivos menos dois). São aceitas apenas máscaras usando /20 ou superior.

   - **Intervalo –** Intervalo de endereços IPv4.
   - **Único** - Endereço IPv4 ou IPv6 únicos. Pode-se usar as formas abreviadas do endereço IPv6, bem como endereços IPv6 referentes a endereços IPv4. No entanto, *não* são aceitos endereços IPv6 anycast, multicast e loopback nem roteamentos padrão.

   Outra opção é clicar no ícone Adicionar vários IPs ( ), acima da seção Definição de intervalo. Copie e cole os endereços IP na caixa de diálogo Importar IPs. Ao clicar em **OK**, pode-se ver os erros realçados em vermelho.
4. Clique em **Novo intervalo de IPs ou endereço IP único** para adicionar outro intervalo, endereço ou máscara de IP, se desejado.
5. Na seção Credenciais, é possível atribuir perfis de autenticação para o intervalo selecionado. Por padrão, todos os perfis de autenticação são selecionados.

   Se você tiver um número grande de perfis de autenticação na lista, é possível digitar o nome de um perfil para filtrar a lista.

   Para exibir apenas os perfis que estão selecionados, clique na caixa de seleção **Ocultar credenciais não usadas**.
6. Quando terminar de definir os intervalos, clique em **Avançar**.

Detecção programada

Na guia Programação, é possível programar a detecção para ser executada no futuro e /ou executar a detecção imediatamente. Você pode programar uma única execução da detecção ou execuções recorrentes.

A detecção programada não interrompe uma detecção que já está em execução. Se, houver uma detecção em execução em andamento quando uma execução de detecção estiver sendo programada, a detecção programada será ignorada.

Se você selecionar **Executar detecção agora** e houver uma detecção em andamento, a execução de detecção atual será encerrada e a nova será executada.

Siga estas etapas para iniciar e/ou programar a detecção:

1. Deixe a caixa de seleção **Executar a detecção agora** selecionada, a menos que não deseje executar a detecção ao concluir o Assistente de detecção.
2. Para programar a detecção, marque a caixa de seleção **Detecção programada**.
3. Insira as informações nos campos de nome e data.

   O campo de hora está no formato de 24 horas. A hora é a hora local do usuário.
4. Para programar execuções de detecção recorrentes, marque a caixa de seleção **Recorrente a cada** e insira o número de horas do intervalo entre as recorrências.
5. Clique em **Concluir** para concluir o Assistente de detecção.

Navegando no Assistente de detecção

Há alguns pontos que devem ser considerados quando se usa o Assistente de detecção:

- Se você clicar no botão **Fechar** ou no ícone de **X** na barra de título antes de concluir o Assistente de detecção, é exibido um prompt perguntando se você deseja salvar as alterações. Se executar a detecção clicando em **Concluir** na última tela do Assistente de detecção, as alterações são retidas.
- Se forem inseridas informações válidas nos campos obrigatórios de um perfil de autenticação ou intervalo de rede, as informações serão salvas automaticamente ao clicar em **Avançar**. Os campos obrigatórios estão destacados em vermelho.
- As senhas dos perfis de autenticação são exibidas como asteriscos. Se desejar ver a senha conforme a for digitando, clique no ícone Mostrar senha ( ) ao lado do campo **Senha**. Após clicar em **Avançar**, a senha será exibida como asteriscos novamente.

Executar a importação com base em arquivo

Usando a importação com base em arquivo, os administradores do CA Nimsoft podem importar informações de dispositivos e de hosts para o CA Nimsoft Monitor sem verificações de rede nem entrada manual. Por não ser necessário verificar o ambiente de TI, a importação de dispositivos com base em arquivo gera menos alertas de segurança e pode ser mais rápida do que detecção automatizada usando o Assistente de detecção.

Observação: se um sistema for detectado por uma verificação automatizada da rede e também incluído em uma importação com base em arquivo, a importação terá precedência. Se as informações sobre o sistema forem diferentes, as informações contidas no arquivo XML para importação com base em arquivo serão aquelas armazenadas no banco de dados.

Siga estas etapas:

1. Crie um arquivo XML contendo informações sobre computadores ou dispositivos de rede.

   Para obter detalhes do conteúdo do arquivo XML, consulte o tópico da ajuda Esquema de arquivo XML (na página 34).

2. Expanda o nó de **Detecção** na exibição em árvore do Gerenciador de serviços unificados.

3. Passe o cursor sobre o nó **Externo** na árvore e clique no ícone de importação ( ) ou clique no nó **Externo** e escolha **Importação da detecção** no menu **Ações**.

4. Navegue até o arquivo XML no navegador de arquivos e clique em **OK**.

   As informações de dispositivos são importados para o banco de dados do Nimsoft. O processamento por discovery_server é iniciado e pode demorar vários minutos ou mais para terminar.

5. Para exibir os dispositivos importados, clique no nó **Externo**.

   Os dispositivos são exibidos na tabela à direita.

Método de importação alternativo:

O probe cm_data_import monitora um diretório para verificar os arquivos XML válidos e, se encontrar um, importa as informações automaticamente para o banco de dados. Veja como o processo funciona:

1. Copie o arquivo XML que você preparou para o diretório <diretório de instalação do Nimsoft>\Probes\Service\cm_data_import\ **import** no sistema que hospeda o probe cm_data_import.
2. O probe cm_data_import verifica esse diretório em intervalos regulares (o padrão é 60 segundos).
3. Se ele encontra um arquivo de importação válido, importa as informações de dispositivos contidas no arquivo para o banco de dados do Nimsoft.
4. O probe move o arquivo para uma subpasta com carimbos de data e hora no diretório <diretório de instalação do Nimsoft>\Probes\Service\cm_data_import**processed**, também no host do probe, e registra os resultados do processo.

Exibir sistemas detectados

O nó de **Detecção** na exibição em árvore do Gerenciador de serviços unificados permite ver os computadores e dispositivos que foram detectados na rede.

A seção Detecção da árvore contém agentes de detecção, com intervalos de rede sob cada agente de detecção. A árvore também tem um nó Automático e um nó Externo.

Os ícones ao lado dos nós da árvore ajudam a identificar o tipo de nó e também fornecem informações adicionais:

- Agente de detecção ou nó de Detecção de nível superior.

– Intervalo da rede.

- Automático. Alguns probes detectam sistemas automaticamente, e esses sistemas são exibidos nesse nó.

- Externo. Os sistemas listados sob esse nó foram importados por meio de detecção com base em arquivo.

- A detecção é programada. Passe o cursor sobre o ícone para ver a hora da próxima execução programada na dica de ferramenta.

- Detecção em andamento. A proporção de azul indica o andamento da detecção.

- Sem detecção programada.

Clique em um nó da árvore para ver os sistemas associados e suas propriedades na tabela à direita. Para exibir as propriedades de todos os sistemas detectados, clique no nó de **Detecção**.

Um gráfico de torta acima da tabela exibe informações sobre os sistemas detectados referentes ao nó selecionado. Escolha outro critério (**Tipo de dispositivo**, **Sistema operacional** etc.) no menu suspenso para alterar os dados exibidos no gráfico.

Clique em uma fatia do gráfico ou em um item da legenda para filtrar por esses sistemas. Apenas os sistemas representados na fatia são exibidos na tabela e refletidos nos links de resposta à direita. Clique novamente na fatia ou no item da legenda para limpar o filtro.

Os links de resposta à direita do gráfico de pizza listam os sistemas considerando há quanto tempo eles responderam a uma solicitação do agente de detecção. Clique em um desses links, como **Recente (último dia)**, para filtrar por esses sistemas. Apenas os sistemas são exibidos no gráfico de pizza e na tabela. Clique novamente no link para limpar o filtro.

Observação: os sistemas que não responderem serão eliminadas do banco de dados. Por padrão, 30 dias após a última resposta de um sistema, o sistema é excluído do banco de dados.

Um campo Filtro rápido abaixo dos links de resposta permite filtrar pelo texto nas colunas **Nome**, **Endereço IP**, **Domínio**, **Nome do SO** e **Origem** da tabela.

Clique no cabeçalho de uma coluna para classificar a tabela pela coluna.

Um ícone de chave ( ) na tabela indica que um agente de detecção não conseguiu autenticar no sistema usando um dos perfis de autenticação definidos. Passe o cursor sobre o ícone de chave para exibir o tipo e o nome do perfil de autenticação usado.

É possível exportar os dados de um agente de detecção ou intervalo de rede. Os dados incluem mais colunas do que as exibidas na tabela Inventário. Os dados são exportados para um arquivo .csv, que é salvo em um local de sua escolha. Para exportar os dados, clique em um agente de detecção ou intervalo de rede na árvore e selecione **Exportar grupo** no menu **Ações**.

Observação: ao escolher **Exportar grupo**, todos os sistemas referentes ao agente de detecção ou intervalo de rede selecionado são exportados, mesmo que a visualização na Exibição de inventário tenha sido filtrada.

Apêndice A: Configuração avançada

Observação: as configurações de verificação da detecção automática, como intervalos da rede e os perfis da credencial de autenticação, são configuradas no Assistente de detecção que é executado no portlet USM no UMP. Para obter informações, consulte a seção sobre o Assistente de detecção (na página 16).

Esta seção contém os seguintes tópicos:

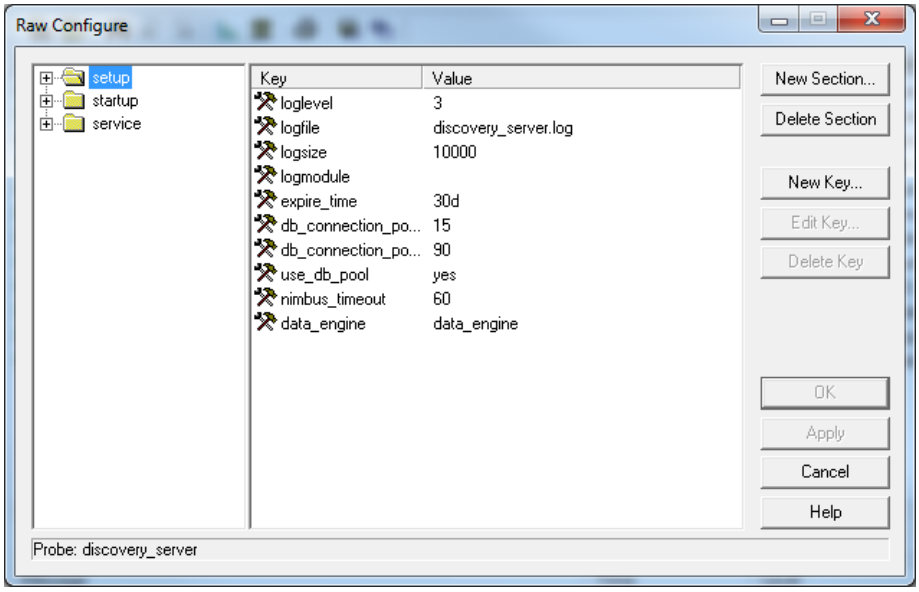
Executando o discovery_server em um robô que não o hub principal (na página 29)
Configurando o tamanho máximo da pilha do Java (na página 30)
Referência de importação com base em arquivo (na página 32)

Executando o discovery_server em um robô que não o hub principal

Por padrão, o servidor de detecção é executado no hub principal, que é o mesmo robô onde o probe data_engine estiver em execução. O servidor de detecção pode ser executado em outro robô, desde que o servidor de detecção possa se comunicar com o probe data_engine e o servidor de banco de dados em seu novo local. Para executar o servidor de detecção em um robô que não o hub principal, siga estas etapas:

1. Desative ou exclua o servidor de detecção no hub primário hub. É possível implantar apenas uma instância do servidor de detecção.
2. No Gerenciador de infraestrutura, clique com o botão direito no probe discovery_server no hub secundário. No Console de administração, clique no ícone ao lado de discovery_server no hub secundário.
3. Selecione Configuração de dados brutos.

4. Na janela de conteúdo, navegue até configuração > chave data_engine e clique no botão Editar chave. No Console de administração, clique no campo do valor para editá-lo.



5. Especifique o endereço completo do probe data_engine completo (*/domínio/hub_principal/robô_principal*/data_engine). É possível pesquisar o endereço de data_engine no Gerenciador de infraestrutura, na categoria SLM no hub principal.

6. Ative ou reinicie o discovery_server em seu novo local.

Configurando o tamanho máximo da pilha do Java

O tamanho máximo padrão da pilha Java para os probes discovery_server e discovery_agent probes é definido pela opção Configuração de dados brutos.

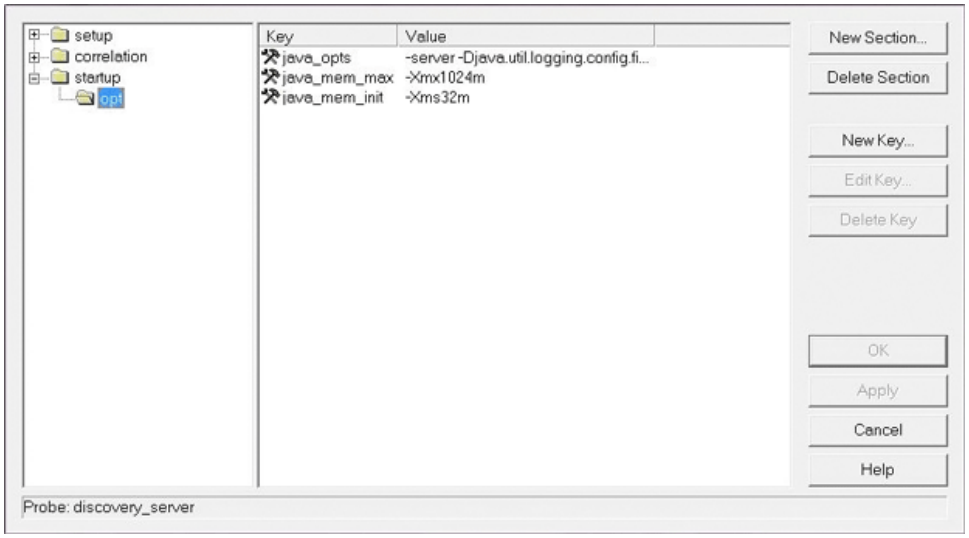
Servidor de detecção

O tamanho padrão máximo da pilha do Java é de 1 GB e oferece suporte a até 5 mil robôs. Para sistemas com mais de 5 mil robôs, o tamanho máximo da pilha do Java deve ser aumentado em um 1 GB para cada 5 mil robôs adicionais.

Exemplo: 2 GB para 5001 a 10 mil robôs; 3 GB para 10001 a 15 mil robôs.

Para definir o tamanho máximo da pilha do Java:

1. No Gerenciador de infraestrutura, mantenha a tecla Shift pressionada e clique com o botão direito do mouse no probe discovery_agent, e selecione **Configuração de dados brutos**. No Console de administração, clique no ícone ao lado de discovery_agent e selecione **Configuração de dados brutos**.
2. Navegue até a **inicialização** e abra **opt**.
3. Na janela de conteúdo, selecione **java_mem_max**. No Gerenciador de infraestrutura, clique no botão **Editar chave**. No Console de administração, clique no campo do valor para editá-lo.



4. Insira o novo valor usando incrementos de 1024 MB.
   - 1 GB = -Xmx1024m
   - 2 GB = -Xmx2048m

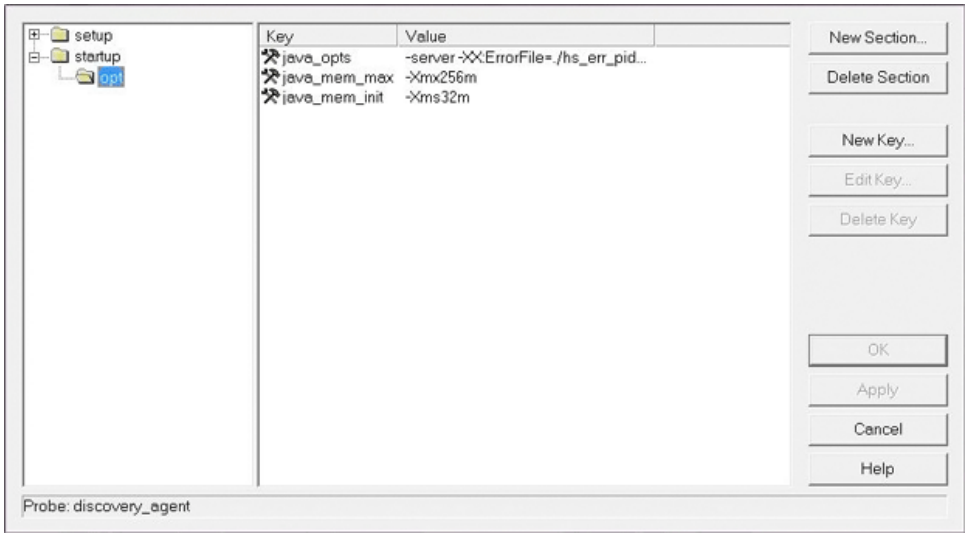
Agente de detecção

O tamanho padrão máximo da pilha do Java tamanho é definido em 256 MB. Para intervalos de detecção muito grandes (equivalentes a uma sub-rede classe B ou mais de 30 mil dispositivos endereçáveis), recomenda-se aumentar a alocação máxima de alocação pilha para 512 MB ou 1024 MB.

Para definir o tamanho máximo da pilha do Java:

1. No Gerenciador de infraestrutura, mantenha a tecla Shift pressionada e clique com o botão direito do mouse no probe discovery_agent, e selecione **Configuração de dados brutos**. No Console de administração, clique no ícone ao lado de discovery_agent e selecione **Configuração de dados brutos**.
2. Navegue até a **inicialização** e abra **opt**.

3. Na janela de conteúdo, selecione **java_mem_max**. No Gerenciador de infraestrutura, clique no botão **Editar chave**. No Console de administração, clique no campo do valor para editá-lo.



4. Insira o novo valor.
   - 512 MB = -Xmx512m
   - 1 GB = -Xmx1024m

Referência de importação com base em arquivo

A função de detecção *importação com base em arquivo* fornece uma maneira prática para importar dados de descrição do dispositivo no banco de dados de detecção. A importação com base em arquivo fornece uma alternativa à detecção automática para preencher o inventário de detecção, sem ter de gerar verificações sobressalentes do ambiente de TI.

O probe cm_data_import processa os dados do dispositivo incluídos em um arquivo XML. Inicie o processo com um destes métodos:

Método 1

1. Abra um navegador de arquivos do nó externo do Assistente de detecção no USM.
2. Navegue até o arquivo XML preparado no sistema de arquivos local para processá-lo e clique em **OK**.
3. O arquivo é processado. Quando o processamento é concluído:
   - Os dispositivos são publicados no barramento da Nimsoft. O discovery_server recebe essa informação e adiciona os dispositivos ao banco de dados de dispositivos.
   - Os dispositivos são exibidos no USM.

Método 2

1. Copie um arquivo XML no diretório *<Nimsoft>\Probes\Service\cm_data_import\import*, no sistema que hospeda o probe cm_data_import.
2. O probe cm_data_import reconhece os novos arquivos e os processa. Esse probe verifica o diretório a intervalos configuráveis (o padrão é 60 segundos). Quando o processamento é concluído:
   - cm_data_import move o arquivo para uma subpasta com indicação de data e hora em *<Nimsoft>\Probes\Service\cm_data_import\processed*.
   - O resultado do processo é registrado.
   - O probe publica os dispositivos no barramento da Nimsoft. O discovery_server recebe essa informação e adiciona os dispositivos ao banco de dados de dispositivos.
   - Os dispositivos são exibidos no USM.

Os dispositivos ficam visíveis na interface do USM em Grupos ou na ramificação **Externo** da Árvore de detecção.

Observação: os dispositivos importados pela importação com base em arquivo não estão refletidos na topologia da Nimsoft.

Esquema de arquivo XML

Esta seção descreve como criar um arquivo XML para usar com a detecção com base em arquivos.

O arquivo XML deve incluir estas propriedades obrigatórias para cada host ou dispositivo:

- PrimaryIPv4Address – Lista o endereço IPv4. Embora o marcador PrimaryIPv6Address exista, os endereços IPv6 não são suportados pela detecção no momento.
- Origem - É importante definir a origem corretamente. Consulte os detalhes na propriedade Origin, na tabela a seguir.

Aqui está um exemplo de XML que ilustra como importar um dispositivo com o endereço IP 1.2.3.4 e a origem "MyOrigin" no banco de dados.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<DevicesToImport xmlns="http://nimsoft.com/2012/11/cm-data-import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <Device>
                <PrimaryIPV4Address>1.2.3.4</PrimaryIPV4Address>
                <Origin>myOrigin</Origin>
        </Device>
</DevicesToImport>
```

Outras propriedades opcionais podem ser incluídas, conforme mostrado no exemplo a seguir. Também é possível localizar esse arquivo de exemplo, denominado example1MaximalDevice.xml, no diretório <diretório de instalação do Nimsoft>\Probes\Service\cm_data_import**schema**, localizado no sistema que hospeda o proble cm_data_import - normalmente o hub principal.

```
  <?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
  <DevicesToImport xmlns="http://nimsoft.com/2012/11/cm-data-import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <Device>
              <Origin>myOrigin</Origin>
              <Label>myComputer</Label>
              <Description>descrição de myComputer deve ser inserida aqui</Description>
              <PrimaryDnsName>myComputer.myCompany.com</PrimaryDnsName>
              <PrimaryIPV4Address>1.2.3.4</PrimaryIPV4Address>
              <PrimaryIPV6Address>fe80::223:ebff:fe06:9d40%10</PrimaryIPV6Address>
              <PrimaryMacAddress>F0-4D-A2-25-5B-7A</PrimaryMacAddress>
              <PrimaryOSType>WindowsServer-2008</PrimaryOSType>
              <PrimaryOSVersion>6.1.7601</PrimaryOSVersion>
              <ProcessorType>x86-64</ProcessorType>
              <Vendor>Dell Inc.</Vendor>
              <Model>PowerEdge T620</Model>
              <PhysSerialNumber>123-456-789-ABCD</PhysSerialNumber>
              <PrimaryDeviceRole>VirtualMachine</PrimaryDeviceRole>
              <PrimarySoftwareRole>DatabaseServer</PrimarySoftwareRole>
              <DBServerType>MSSQLServer</DBServerType>
              <WmiAuthId>3</WmiAuthId>
              <ShellAuthId>5</ShellAuthId>
              <SnmpAuthId>7</SnmpAuthId>
              <AppServerType>Unknown</AppServerType>
              <VirtualizationEnvironment>VMware</VirtualizationEnvironment>
              <MonitorFrom>monitoringRobotHostName</MonitorFrom>
       </Device>
</DevicesToImport>
```

A tabela a seguir descreve as propriedades de XML. No caso de propriedades que se referem a enumerações abertas, navegue até <caminho de instalação do Nimsoft>\Probes\Service\cm_data_import**schema** e abra **usm-openenums.xml** ou **cm-data-import-openenums.xml** para exibir os valores definidos para cada instância de enumeração. É altamente recomendável usar os valores definidos pelas enumerações abertas, embora isso não seja rigorosamente necessário.

Para implantar um robô em um sistema importado usando USM e ADE, são necessárias algumas propriedades adicionais além do endereço IP e da origem. Elas são explicadas na tabela a seguir.

Propriedade	Obrigatório?	Descrição
Origin	Sim	Os dados de QoS de probes são marcados com um nome de origem para identificar sua origem. O padrão de nome de origem será o nome do hub Nimsoft, mas ele pode ser substituído no hub ou robô (controlador) para separar os dados em um ambiente de multilocação. Para garantir que os dados de QoS de probes sejam correlacionados ao dispositivo, o nome de origem especificado aqui deve corresponder ao nome de origem que você pretende usar na Infraestrutura de hubs e robôs do Nimsoft.
Label	Não	Uma breve descrição ou legenda.
Descrição	Não	Descrição textual do dispositivo.
PrimaryDnsName	Não	O DNS da entidade, que pode ser usado para correlação.
PrimaryIPV4Address	É obrigatório um endereço IPv4	Um endereço IPv4 para a entidade que pode ser usado para fins de correlação e identidade.
PrimaryIPV6Address	Não	Um endereço IPv6 para a entidade que pode ser usado para fins de correlação e identidade. O endereço é expresso usando a notação formal e completa de IPv6 (8 grupos de até 4 dígitos hexadecimais, usando somente letras maiúsculas quando aplicável, separados por dois-pontos).
OtherIPAddresses	Não	Uma entidade pode ter vários endereços IP. Este elemento captura os valores desses endereços, enquanto os elementos do PrimaryIPAddress são projetados para serem usados para fins de correlação e identidade. Os diversos valores são separados por vírgulas. Os valores IPv4 ou IPv6 podem ser especificados, mas os endereços devem ser formatados seguindo os padrões regex definidos por usm-core:IPV4AddressFormat ou usm-core:IPV6AddressFormat.
PrimaryMacAddress	Não	Um endereço MAC para a entidade que pode ser usado para fins de correlação e identidade. O endereço é expresso como 6 grupos de 2 dígitos hexadecimais (usando somente letras maiúsculas), separados por traços.

Propriedade	Obrigatório?	Descrição
OtherMacAddress	Não	Uma entidade pode ter vários endereços MAC. Este elemento captura os valores desses endereços, enquanto o elemento do PrimaryMacAddress é projetado para ser usado para fins de correlação. Os diversos valores são separados por vírgula e são formatados seguindo o padrão regex definido por usm-core:MacAddressFormat.
PrimaryOSType	Exigido por ADE para a implantação de robôs	Tipo de sistema operacional definido pela enumeração aberta OSTypeEnum. No caso do Linux, o nome da distribuição do Linux é exigido pelo ADE (por exemplo, **Linux-RedHat**).
PrimaryOSVersion	Não	Detalhes da versão do sistema operacional.
ProcessorType	Exigido por ADE para a implantação de robôs	Ambiente/tipo de processador (por exemplo, x86) conforme definido pela enumeração aberta - ProcessorEnvironmentEnum.
Vendor	Não	O nome do fornecedor/fabricante do hardware, como definido pela enumeração aberta VendorEnum.
Model	Não	Nome/número do modelo do hardware.
PhysSerialNumber	Não	Uma sequência de caracteres de identificação atribuída pelo fabricante do hardware e impressa em uma etiqueta fixada ao componente. Os dados desse elemento devem ser inseridos diretamente da etiqueta do fabricante no componente (que pode ser uma etiqueta RFID) ou lida no campo entPhysicalSerialNum de Entity-MIB do SNMP. Uma entidade virtual NÃO tem um PhysSerialNumber.
PrimaryDeviceRole	Não	A função do dispositivo conforme definida pela enumeração aberta DeviceRoleEnum.
PrimarySoftwareRole	Não	A função do software conforme definida pela enumeração aberta SoftwareRoleEnum.
DBServerType	Não	O tipo de servidor de banco de dados do qual essa é uma instância, definido pela enumeração aberta DBServerTypeEnum.
AppServerType	Não	O tipo de servidor de aplicativos, como definido pela enumeração aberta AppServerTypeEnum.

Propriedade	Obrigatório?	Descrição
VirtualizationEnvironment	Não	O valor que indica o ambiente de virtualização específico (gerenciador de hipervisor) de um hipervisor ou sistema virtual. Os valores são definidos na enumeração aberta VirtualizationTypeEnum.
WmiAuthId	WmiAuthId ou ShellAuthID é exigido pelo ADE para implantação por robô	Uma ID de perfil de identificação definida pelo Nimsoft a ser usada para acesso WMI. Este é o campo de ID no perfil de autenticação WMI.
ShellAuthId	WmiAuthId ou ShellAuthID é exigido pelo ADE para implantação por robô	Uma ID de perfil de identificação definida pelo Nimsoft a ser usada para acesso SSH ou telnet. Este é o campo de ID no perfil de autenticação de Shell.
SnmpAuthId	Não	Uma ID de perfil de identificação definida pelo Nimsoft a ser usada para acesso SNMP. Este é o campo de ID no perfil de autenticação SNMP.
MonitorFrom	Não	Se o dispositivo será monitorado remotamente, especifica o sistema a partir do qual o dispositivo deverá ser monitorado. O valor pode ser especificado como um endereço IP, nome de host simples, nome de domínio totalmente qualificado ou o endereço do Nimsoft (/NimsoftDomain/HubName/RobotName). Um robô do Nimsoft deve ser instalado no sistema especificado aqui. Se o robô não estiver instalado, o dispositivo não será importado. O nome da origem usada pelo robô deve corresponder à origem especificada para o dispositivo; desse modo, há garantia de que os dados de QoS de probes sejam correlacionados ao dispositivo.